IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPEAL NO:

In Re Application of: Paul A. CRONCE et al.

Confirmation No.: 1789

Serial No.: 10/080,639

Filed: February 21, 2002

For: DELIVERY OF A SECURE SOFTWARE LICENSE FOR A SOFTWARE PRODUCT AND A TOOLSET FOR CREATING THE SOFTWARE PRODUCT

APPEAL BRIEF

Stephen G. Sullivan
Attorney for Appellants
Strategic Patent Group, P.C.
P.O. Box 1329
Mountain View, CA 94042

TOPICAL INDEX

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In Re Application of:	Date: October 31, 2005
Paul A. CRONCE	Confirmation No.: 9753
Serial No.: 10/080,639	Group Art Unit: 3621
Filed: February 21, 2002	Examiner: Bayat, Bradley B.

For: DELIVERY OF A SECURE SOFTWARE LICENSE FOR A SOFTWARE PRODUCT AND A TOOLSET FOR CREATING THE SOFTWARE PRODUCT

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

Appellant herein files an Appeal Brief drafted in accordance with the provisions of 37 C.F.R. §41.37 as follows:

I REAL PARTY IN INTEREST

Appellant respectfully submits that the above-captioned application is assigned, in its entirety to Pace Anti-Piracy of San Jose, CA.

II RELATED APPEALS AND INTERFERENCES

Co-pending application number 10/072,597, entitled “A Method and System for Delivery of Secure Software License Information“ filed on February 5, 2002, and assigned to the assignee of the present invention is also currently under appeal.

III STATUS OF CLAIMS

Application Serial No. 10/080,639 (the instant application), as originally filed, included claims 1-14. Claims 1-14 are presently pending. In response to the Office Action dated June 29, 2005, Claims 1, 5, 7 and 13 were amended. In response to the Final Office Action dated January 23, 2006, claim 7 was amended. Claims 1-14 are on appeal and all applied prospective rejections concerning Claims 1-14 are being appealed herein.

IV STATUS OF AMENDMENTS

The Amendment under Rule 1.116 dated April 24, 2006, submitted in response to the Final Office Action dated January 23, 2006, was not entered by the Examiner (Notice of Abandonment 9/25/2006).

V SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 recites a method for delivery of a license-managed toolset for creating a license-managed software product. Step (a) recites providing an authorization process, that includes (i) creating a first public and private key pair for a software publisher (Specification page 12, line 12; page 13 line 19 through line 20, page 16, line 4, for example) (ii) creating a second public and private key pair for a software program, wherein at least one of the second private and public keys is digitally signed by the first private key of the software publisher (Specification page 16, lines 5-7, for example), (iii) creating an authorization program for the software program, and embedding a copy of the first and second public keys in the authorization program Specification page 16, line 1-14, for example), and (iv) combining the authorization program with a software program (page 8, line 12 through page 9, line 1, for example). When the software program is invoked on a computer, the authorization program obtains a license for the software program by (1) creating a license request, (2) encrypting the license request using the second public key, (3) transmitting the encrypted license request to a key authority, (4) receiving an encrypted license from the key authority, wherein the license includes license terms, and (5) decrypting the license using the first public key, such that the license terms are used to control use of the software program (Specification page 9, line 2-14; page 16, line 18 through page 20, line 4; page 24, line 14 through page 25, line 14, for example).

Step (b) recites implementing the authorization process in a software toolset that is provided by a toolset publisher, wherein when the authorization process is invoked in the software toolset, the toolset publisher is the publisher in the authorization process and the software toolset is the software program in the authorization process (Specification page

23, lines 13-15; page 28, line 13 through page 29, line 14; page 28, line 24 through page 33, line 22 for example).

Step (c) recites implementing the authorization process in a software product that is provided by a publisher of the software product using the software toolset, wherein when the authorization process is invoked in the software product, the publisher of the software product is the publisher in the authorization process and the software product is the software program in the authorization process, whereby both the software toolset and the software product use the same authorization process to obtain respective licenses (Specification, page 32, line 24 through page 35, line 14, for example).

The recitations of independent claim 7 are similar to claim 1 in that a method is also recited for delivery of a license-managed toolset for creating a license-managed software product. However, in step (a)(i) a certificate is created for the software publisher by a certificate authority, and in step (a)(i) a second certificate is created for the software product using the software publishers private key (Specification page 13, line 1-21; page 33, lines 12-22; page 34, lines 16-19, for example). And step (a)(iii) recites embedding a copy of the first and second certificates and second private key in the authorization program (Specification, page 16, lines 2-14).

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-14 stand rejected under 35 U.S.C. §102(e) as being unpatentable over U.S. Patent No. 6,898,706 (Venkatesan).

VII ARGUMENTS

U.S. Patent No. 6,898,706 (Venkatesan) fails to anticipate claims 1-14.

Anticipation requires that a prior art reference disclose each and every claim element of the claimed invention. It is respectfully submitted that Venkatesan fails to teach, or even suggest, each and every element of independent claims 1 and 7.

The present invention provides a method and system for delivery of a licensed toolset to a software publisher for creating license-managed software products. The method comprises providing an authorization process, and implementing the authorization process for both a toolset publisher and related toolset and a software publisher and related software product, whereby the same authorization process is used to obtain respective licenses. The authorization process includes creating a first public and private key pair for the software publisher, and creating a second public and private key pair for the software product, wherein at least one of the second private and public keys is digitally signed by the first private key of the software publisher. An authorization program is also created for the software program that has embedded copies of the first and second public keys. The software program and the authorization program are combined, such that when the authorization program is invoked, the authorization program obtains a license for controlling the use of the software program. The license is obtained by creating a license request, encrypting the license request using the second private key, transmitting the license request to a key authority, receiving a license from

the key authority with license terms, decrypting the license, and using the license terms to control the use of the software program.

Referring now to the independent claims, in claim 1, Applicants refer broadly to private and public key pairs, while in claim 7 Applicants refer to certificates, which usually include other information besides keys. According to the exemplary embodiment, the software program keys are connected to the software publisher keys such that only that publisher can allow the software program to be authorized. To accomplish this, at least one of the keys of the software program is digitally signed by the private key of the publisher. Using the public key of the publisher, the authorization program can verify that the publisher who signed its product public key is the same publisher who signed the license in response to license request.

In independent claim 7, Applicants refer to signed certificates, which have associated private keys. The public keys are part of the certificate. So in this case, the product certificate is digitally signed by the publisher private key. This allows the authorization program to verify that the publisher who signed its product certificate is the same publisher who signed the license.

The publisher of the software program can use a toolset to convert the software program into “a license-managed software product.” The publisher uses the toolset and the publisher certificate to create protected software products and to create product certificates for licensing. Thus, the present invention provides a chain of certificates to authorize use of a software program through a license. To run, a software product has to verify the product certificates. Verification means verifying the certificate chain, meaning that the product certificate is cryptographically tied to the proper publisher

certificate, which in turn, may be cryptographically tied to a certificate authority certificate. The elegance of the solution is that it allows the certificate authority to control how publishers use the toolset, allows publishers to control how their end-users use their protected software products, and prevents one publisher from authorizing a product from another publisher.

In contrast, Venkatesan is directed to techniques for controlling access and use of protected objects by client computer using a digital rights management (DRM) system in the client computer that is based primarily on watermarks being embedded throughout the software object. Applicant acknowledges that Venkatesan may teach a software licensing mechanism, the association of a public and private key pair with a software publisher, and a publisher cryptographically signing a license in response to a license the request. However, despite these teachings, Venkatesan still fails to address the security of the license request and resulting license, as claimed in the present invention for least the following reasons.

However, despite these teachings, Venkatesan still fails to address the security of the license request and resulting license, as claimed in the present invention for least the following reasons. First, although Venkatesan may teach creating a first public and private key pair and a second public and private key pair, Venkatesan fails to teach or suggest “combining the authorization program with a software program,” as recited in step (a) of claims 1 and 7, wherein “when the software program is invoked on a computer,” the authorization program obtains a license for the software program, as recited in step (a)(iv).

Venkatesan fails to teach or suggest that the authorization program creates a license request. Instead, Venkatesan clearly teaches that "the user" initiates the license request with the publisher through the client PC (e.g., a web browser). Example portions of Venkatesan state:

> After a user has downloaded a watermarked object, then, in order to use that object, the user, through his(her) client PC, electronically transacts, through the Internet, with publisher's web server. In return for payment of a specific licensing fee to the publisher, this web server downloads to the client PC an electronic license… (Col. 6, lines 21-27) and (col. 14, lines 35 and 41).

> Subsequently, the user, through client PC_j, establishes an Internet session with the publisher's web server and as, indicated by block 540, electronically transacts with that server to obtain a license to use the previously downloaded object.... Once the user makes the selection and authorizes electronic payment for the desired rights, the browser, based on embedded code in the web page, transmits, to the publisher's web server, the rights selection, payment authorization and a computer identification (CID) associated with client PC_j.... Once this information is transmitted to the publisher's web server, that server issues, as indicated by block 550 shown in FIG. 5, an electronic license (L_i) and transmits, as symbolized by line 555, that license to the client PC. (Col. 21, line 66 through col. 22, line 20).

Accordingly, because the license request is manually initiated by the user by interacting with the PC through a Web browser, Venkatesan fails to teach or suggest that the authorization program, which is combined with the software program, creates the license request upon invocation of the software program.

It should be noted that Venkatesan also provides for an enforcer that looks for watermarks in an object whenever the client computer attempts to access a file containing the protected object. It is also believed that the enforcer cannot be considered analogous to the "authorization program" because the enforcer does not generate a license request. In addition, the enforcer is not part of the protected

software object. Rather, the enforcer is part of a digital rights management (DRM) system, which in turn is part of the operating system (col. 18. lines 44-45).

Consequently, Venkatesan's fails to teach or suggest a method that combines the authorization program with a software program, where "when the software program is invoked on a computer," the authorization program creates "a license request," as recited in claims 1 and 7.

Second, although Venkatesan may teach the use of a publisher key, Venkatesan also fails to teach or suggest "creating a first private and public key for a software publisher", as recited in step (a(i)) of claims 1 and 7. The Examiner makes reference to a "secret key", but Venkatesan describes that this secret key, which is included in the license, "is to decrypt the [software] object. This secret key..., is a symmetric encryption key, i.e., the same key used use by the publisher to encrypt the object (col. 22, lines 25-28). Although Venkatesan's secret key is used to encrypt the software object, and presumably considered by the Examiner to be "created" for the software program, Venkatesan's secret key is "symmetric", i.e., there is only one. Consequently, there can be no pair of keys for the software program, i.e., a product private key and public key. More importantly, it is believed that Venkatesan's secret key is only used to encrypt and decrypt the software object, but not to digitally sign the second private and public keys for a software program by the first private key of the software publisher, as recited in step (a)(ii) of claims 1 and 7.

One of the elements of the present invention is the fact that the license request created by the authorization program is delivered securely to the key authority. The

security is provided by "encrypting the license request using the second public key," as recited in step (a)(iv)(2).

Venkatesan also fails to address providing security for the license request. Venkatesan merely describes that “the user” initiates the license request with the publisher through the client PC (e.g., a web browser), and in return receives a license. Not only is Venkatesan’s license request not encrypted by the second public key for the software program, but the license request appears not to be signed or encrypted all. Consequently, Venkatesan fails to teach or suggest "encrypting the license request using the second public key,” as recited in step (a)(iv)(2).

In the Response to Arguments section of the Final Office Action, the Examiner took issue with Applicant's statement in the previous Amendment that unlike the present invention, in Venkatesan, there is no chaining of certificates. To rebut this argument, the Examiner cited col. 9, lines 25-56 of Venkatesan. However, col. 9, lines 25-56 of Venkatesan make clear that the digital signatures and establishment of chains of trust relate to “components of the O/S and particularly throughout enforcer 600 and DRM system 456,” not between software programs, software publishers, and in some embodiments, certificate authorities, as claimed. Accordingly, Venkatesan fails to teach the cooperation of elements in claim 7 that provide for the delivery of secure software license information.

Therefore, it is respectfully submitted that independent claims 1 and 7 are each allowable over Venkatesan for at least these reasons.

For at least the reasons stated above, Venkatesan fails to teach or suggest each and every claim element of independent claims 1 and 7. Because the secondary

references stand or fall with the primary references, claims are allowable because they are dependent upon the allowable independent claims.

Accordingly, it is respectfully submitted that the §102(e) rejection of claims 1-14 based on Venkatesan has been overcome and that claims 1-14 are patentable. Thus, Appellant respectfully requests that the Board reverse the rejection of all the appealed Claims and find each of these Claims allowable.

Note: For convenience of detachment without disturbing the integrity of the remainder of pages of this Appeal Brief, Appellant's "APPENDIX" sections are contained on separate sheets following the signatory portion of this Appeal Brief.

Respectfully submitted,
STRATEGIC PATENT GROUP

March 19, 2007
Date

/Stephen G. Sullivan/
Stephen G. Sullivan
Attorney for Appellant(s)
Reg. No. 38,329
(650) 493-4540

VIII CLAIMS APPENDIX

1 (Previously Presented) A method for delivery of a license-managed toolset for creating a license-managed software product, the method comprising the step of:

(a) providing an authorization process, the authorization process including the steps of:

(i) creating a first public and private key pair for a software publisher,

(ii) creating a second public and private key pair for a software program, wherein at least one of the second private and public keys is digitally signed by the first private key of the software publisher,

(iii) creating an authorization program for the software program, and embedding a copy of the first and second public keys in the authorization program,

(iv) combining the authorization program with a software program, such that when the software program is invoked on a computer, the authorization program obtains a license for the software program by:

(1) creating a license request,

(2) encrypting the license request using the second public key,

(3) transmitting the encrypted license request to a key authority,

(4) receiving an encrypted license from the key authority, wherein the license includes license terms, and

(5) decrypting the license using the first public key, such that the license terms are used to control use of the software program;

(b) implementing the authorization process in a software toolset that is provided

by a toolset publisher, wherein when the authorization process is invoked in the software toolset, the toolset publisher is the publisher in the authorization process and the software toolset is the software program in the authorization process, and

(c) implementing the authorization process in a software product that is provided by a publisher of the software product using the software toolset, wherein when the authorization process is invoked in the software product, the publisher of the software product is the publisher in the authorization process and the software product is the software program in the authorization process, whereby both the software toolset and the software product use the same authorization process to obtain respective licenses.

2 (Original) The method of claim 1 further includes the step of transferring the first and second private keys to a key authority for receiving license requests and generating licenses.

3 (Original) The method of claim 1 further includes the step of including product and customer information within the license request and license documents.

4 (Original) The method of claim 1 further includes the step of associating the license request with a financial transaction, and incorporating financial transaction information within the license.

5 (Original) The method of claim 1 further includes the steps of:

(a) assigning a publisher ID to the publisher,

(b) embedding the publisher ID within the authorization program,

(c) including the publisher ID within the license, and

(d) comparing the embedded publisher ID with the publisher ID within the license to verify the publisher of the software program to be authorized has generated the license.

6 (Previously Presented) The method of claim 1 further including the steps of:

(a) generating a machine fingerprint within the authorization process,

(b) incorporating the machine fingerprint within the license request,

(c) incorporating the machine fingerprint within the license terms, and

(d) using by the authorization program the machine fingerprint to prevent use of the software product on a different machine than the one which made the license request.

7 (Previously presented) A method for deliverly of a license-managed toolset for creating a license-managed software product, the method comprising the step of:

(a) providing an authorization process, the authorization process including the steps of:

(i) creating a first public and private key pair for a software publisher, and creating a first certificate with the public key using a certificate authority,

(ii) creating a second public and private key pair for a software program, and creating a second certificate with the software publisher private key, wherein at least one of the second private and public keys is digitally signed by the first private key of the software publisher.

(iii) creating an authorization program for the software program, and embedding a copy of the first and second certificates and second private key in the authorization program,

(iv) combining the authorization program with a software program, such that when the software program is invoked on a computer, the authorization program obtains a license for the software program by:

(1) creating a formatted license request,

(2) signing the formatted license request using the second public key,

(3) transmitting the signed formatted license request to a key authority,

(4) receiving an signed formatted license from the key authority, wherein the license includes license terms, and

(5) validating the license using the first certificate, such that the license terms are used to control use of the software program;

(b) implementing the authorization process in a software toolset that is provided by a toolset publisher, wherein when the authorization process is invoked in the software toolset, the toolset publisher is the publisher in the authorization process and the software toolset is the software program in the authorization process, and

(c) implementing the authorization process in a software product that is provided

by a publisher of the software product using the software toolset, wherein when the authorization process is invoked in the software product, the publisher of the software product is the publisher in the authorization process and the software product is the software program in the authorization process, whereby both the software toolset and the software product use the same authorization process to obtain respective licenses.

8 (Original) The method of claim 7 further includes the step of including product and customer information within the license request and license documents.

9 (Original) The method of claim 7 further includes the step of associating the license request with a financial transaction, and incorporating financial transaction information within the license.

10 (Original) The method of claim 7 further includes the step of formatting the license request and license using a proposed signed XML document format.

11 (Original) The method of claim 7 further includes the step of generating the first public and private key pair for the software product publisher during the authorization process for the toolset, using the steps of:

(a) creating the first public and private key pair for the software publisher prior to using the authorization process for the toolset;

(b) including the public key within the license request document in the form of a

certificate request;

(c) receiving the certificate within the license document, and

(d) using the received certificate in conjunction with the private key as the first key pair in the authorization process for the software product.

12 (Original) The method of claim 7 further includes the step of transferring the first and second private keys and certificates to a key authority for receiving license requests and generating licenses.

13 (Original) The method of claim 7 further includes the steps of:

(a) assigning a publisher ID to the publisher,

(b) including the publisher ID within the publisher certificate, included within the software product license,

(c) embedding the publisher ID within the authorization program,

(d) comparing the embedded publisher ID with the publisher ID within the certificate to verify the publisher of the software program to be authorized has generated the license.

14 (Previously Presented) The method of claim 7 further including the steps of:

(a) generating a machine fingerprint within the authorization process,

(b) incorporating the machine fingerprint within the license request,

(c) incorporating the machine fingerprint within the license terms, and using by the authorization program the machine fingerprint to prevent use of the

software product on a different machine than the one which made the license request.

IX EVIDENCE APPENDIX

(None)

X RELATED PROCEEDINGS APPENDIX

(None)